PHILANTHROPIC SOLUTIONS

Protecting Your Nonprofit From Fraud

While our daily headlines tend to focus on high-profile cases of fraudulent activity impacting large corporations, it may be surprising that nonprofit organizations are even more susceptible to this particular crime.

Nonprofits are here to serve. They often do so on tight budgets with small staffs who are laser-focused on fulfilling missions and enriching communities. But in today's world, nonprofits are often targeted by criminal entities who see them as soft targets with sensitive information about donors and constituents. Indeed, a recent study by the Association of Certified Fraud Examiners (ACFE) shows that nearly one out of 10 nonprofits are victims of fraud every year, with an average loss of $75,000.

Nonprofits have the potential for higher risk than for-profit companies because nonprofits often lack the financial and human resources to protect against such malfeasance. Nonprofits are under pressure to deploy money and human capital as efficiently as possible. This can lead some nonprofits to be reluctant to expend the necessary resources on fraud protection, resulting in nonprofits being a target of fraud.

The ACFE study shows that the top three vulnerabilities for fraud detection within nonprofits include a lack of internal controls (35 percent), lack of management review (19 percent) and override of existing controls (14 percent).

The same study shows the most common perpetrators of fraud within an organization are executives (39 percent of cases with a median loss of $250,000); managers (35 percent of cases with a median loss of $95,000) and employees (23 percent of cases with a median loss of $21,000.)

Case Study

The following scenario is typical of how fraud can evolve within a nonprofit organization:

> *Mark was a recent university accounting graduate. Prior to sitting for his CPA exam, he wanted to gain some practical experience in accounting, so he decided to take a gap year and go to work with a nonprofit in his hometown.*
>
> *Mark's skills quickly proved his value to the nonprofit executives and, as his gap year came to a close, he was recommended to the Board to oversee the financial operations of the organization. Everyone liked Mark and respected his credentials, values, and skill, and awarded him the responsibility.*
>
> *After a few months in his new role, Mark began to have trouble making ends meet. His salary at the organization just wasn't enough to cover all his expenses, and with his student loans coming due, his financial condition began to deteriorate.*

> *Mark controlled the receipt, approval, and payment of invoices, and had full control over the financial operations, including the reconcilement of credit card and bank statements. His fraudulent activities began small and started with small credit card purchases for gas, groceries, and food. At first, he repaid these purchases before they posted to the credit card statements, but he quickly realized that no one noticed.*
>
> *Once he realized his power and opportunity, the purchases increased. He also began creating invoices from fictitious suppliers and writing checks to pay the invoices. He would remove both the invoice and the check from the ledger during the reconcilement process. At the end of the year, his report to the Board was falsified to cover his actions.*
>
> *Over a few years, his fraud continued to grow, and by the time someone began to ask questions, he had amassed nearly a million dollars in fraudulent payments stolen from the organization.*
>
> *Cases like this occur at nonprofit organizations more often than you might think. The impact to the nonprofit often extends beyond the dollar amount of the fraud perpetuated. For example, the fraud can harm the nonprofit's reputation, making it harder to raise funds from its existing donor base as well as to attract new donors. The potential financial and reputational risk provide even more motivation to understand the importance of evaluating your controls and payment processes.*

Other Fraudulent Activities Impacting Nonprofits

One of the key scams that impact nonprofits is also one of the oldest - check fraud, which makes up almost 80% of fraud activity (included in this is also debit cards). It's important to understand that a check contains, names, addresses, bank account numbers and routing numbers which are all easy ways for potential fraud activity should the check get into the hands of the wrong person. According to Jeff Taylor, head of Commercial Fraud Forensics at Regions, fraudsters can "wash" or alter existing checks, create counterfeits using blank check stock or use forgery to steal money from a nonprofit organization.

Taylor recommends five best practice tips to combat check fraud:

1. Reconcile accounts in a timely fashion in order to spot abnormal activity.
2. Place stop payment on any checks that have been lost or stolen.
3. Convert paper payments to electronic payments whenever possible.
4. Securely store check stock, deposit slips and bank statements, then destroy securely.
5. Use Positive Pay with Payee Name Verification, a powerful tool that sends information to your bank that matches what's written with what's coming in.

"You want to convert to electronic payments anytime you can because it gives you more control over your transaction," cites Taylor.

Another growing fraud area, according to Taylor, is **ransomware,** the practice whereby fraudsters target an organization by placing malware on the organization's computer system and locking the system with encryption tools.

In such instances, payment (ransom) is demanded before the fraudster releases the code to unlock the system.

Fraudsters access a computer system through a number of tactics, including phishing and social engineering, infected software applications, documents, files and external storage devices, as well as through compromised websites.

Additionally, **business email compromise** is on the rise and something nonprofits need to pay special attention to.

Executive email intrusion is a common tactic in which a criminal impersonates a senior executive requesting that a payment be sent or giving an order to purchase gift cards.

Similarly, **vendor email intrusion** takes place when a criminal impersonates a vendor requesting the company to change payment remittance information.

And **employee email intrusion** takes place when a criminal impersonates an employee requesting the vendor to send payment account information. To clarify: this fraud attack method includes the request for disclosure of payment information, but also includes the impersonation of the employee to redirect payments owed to the employee for payroll or expense reimbursements.

Safeguarding Recommendations

At Regions, we recommend the following steps to take to ensure long-term safety:

Guard your house with IT best practices – Conduct an IT vulnerability assessment, create effective firewalls, and regularly patch and update security systems while routinely backing up critical data. Require the use of secure passwords and multi-factor authen-tication. And leverage fraud protection tools including Positive Pay, ACH Positive Pay and Account Reconciliation.

Create Associate and Volunteer Training Program(s) – Conduct training programs for associates and any volunteers with access to your data, network or sensitive systems, emphasiz-ing password management. Educate critical payment stream associates and volunteers, perform regular phishing testing, encourage associates and volunteers to be aware of potential points of compromise and remind them not to click on links or attachments from unknown sources. Turnover of associates and volunteers may be high, so it is important to conduct regular, repeated training. For great videos and information on education programs, visit regions.com/stop fraud or regions.com/fraudprevention.

Create a Fraud and Risk Governance Plan – Identify and document risk tolerance, create a robust vendor management program, document a detailed fraud response plan and review cybersecurity insurance coverage. Nonprofits should also divide financial responsibilities and review and establish internal controls, such as a call-back procedure for changes in payments.

Other Best Practices:

Implement board oversight

An increasing number of nonprofits are not only elevating fraud and cybersecurity to board level discussions, but they are also creating board committees to address the issues in a more proactive and strategic manner. Encouraging board involvement and oversight can foster a culture of risk mitigation. As a result of these and other actions, we're also seeing more nonprofits obtain cyber or fraud insurance, a practice that will likely increase in coming years.

Encourage employees to speak up if unusual activity is noticed

More and more nonprofits today are focused on creating a transparent work environment by developing an anti-fraud policy and implementing a fraud hotline. Such policies provide a guide for ethical behavior and may help employees be more vocal if fraudulent activity is detected. Hotlines serve an equally important role as more than 40 percent of fraud tips come from this type of employee reporting.

Review your current control environment

A typical best practice involves segregating duties as much as possible. The goal should be to have at least two people involved in every transaction, and the person performing reconciliations should not have access to the assets being reconciled. Additionally, if the executive director has little or no supervision over transactions, consider having someone from the board of directors or the audit or finance committee be responsible for such oversight.

Create ongoing monitoring procedures

Another common best practice involves the implementation of monitoring procedures for critical or high-risk business processes, such as performing a monthly review of payroll changes or credit card refunds. Monitoring activities can help identify suspicious activity early on and are critical when there is limited segregation of duties.

The perception of detection is a strong deterrent to fraud. Making employees aware that monitoring activities are being performed without providing further details, such as when the monitoring will take place, has proven to be effective for many organizations. If your nonprofit is large enough, consider creating an internal audit function or department that can help in performing some of these activities.

Summary

Nonprofits provide essential services to support our communities and they do so by dedicating nearly all their resources to their mission. Despite their critical missions, nonprofits are not immune to fraud.

Given the financial and reputational risks associated with fraud, it is imperative that nonprofits focus on implementing safeguards to reduce fraud risk. All efforts should start at the top so that the management team and board members are aware of the circumstances and pressures that often lead to fraudulent activity both inside and outside the organization. For additional tips and resources on fraud awareness and prevention, visit regions.com/stop fraud or regions.com/fraudprevention.

REGIONS

Investment, Insurance and Annuity Products:
Are Not FDIC Insured | Are Not a Deposit | May Go Down in Value | Are Not Bank Guaranteed
Are Not Insured by Any Federal Government Agency | Are Not a Condition of Any Banking Activity

The information presented is general in nature and should not be considered, legal, accounting or tax advice. Regions reminds its customers that they should be vigilant about fraud and security and that they are responsible for taking action to protect their computer systems. Fraud prevention requires a continuous review of your policies and practices, as the threat evolves daily. There is no guarantee that all fraudulent transactions will be prevented or that related financial losses will not occur. Visit regions.com/STOPFRAUD, or speak with your Banker for further information on how you can help prevent fraud.